

# 安全-RSA (BUUCTF)

原创

小狐狸FM  于 2021-08-09 17:19:16 发布  170  收藏

分类专栏: [安全 # CTF夺旗](#) 文章标签: [python rsa](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/smallfox233/article/details/119542322>

版权



[安全](#) 同时被 2 个专栏收录

91 篇文章 9 订阅

订阅专栏



[CTF夺旗](#)

38 篇文章 0 订阅

订阅专栏

## 文章目录

[前言](#)

[一、题目](#)

[二、WriteUp](#)

## 前言

如果安装 `gmpy2` 的时候报错, 可以看下方的文章

[Python-解决下载gmpy2的报错问题](#)

[安全-RSA算法基础](#)

## 一、题目

[题目链接](#)

题目

解题快手榜

×

# RSA

## 1

注意：得到的 flag 请将 noxCTF 替换为 flag，格式为 flag{} 提交。

70a2f2f0-d...

Flag

提交

<https://blog.csdn.net/smallfox233>

题目.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

在一次RSA密钥对生成中，假设 $p=473398607161$ ， $q=4511491$ ， $e=17$   
求解出 $d$ 作为flag提交

<https://blog.csdn.net/smallfox233>

## 二、WriteUp

RSA的公式如下：

$$n = p * q$$

$$\varphi(n) = (p-1) * (q-1)$$

$$c = (m^e) \bmod n$$

$$d = 1 \bmod \varphi(n) / e$$

$$m = (c^d) \bmod n$$

<https://blog.csdn.net/smallfox233>

- 其中已知的三个量是  $e$ 、 $p$  和  $q$ ，所以可以先计算欧拉函数再计算  $d$  的值
- 先算出欧拉函数  $\phi(n)$  的值，然后调用 `gmpy2` 的库实现  $1 \bmod \phi(n) / e$

```
p:473398607161
q:4511491
e:17
125631357777427553
>>> |
https://blog.csdn.net/smallfox233
```

```
# coding=utf-8
# 作者: 小狐狸FM
import gmpy2
p = int(input("p:"))
q = int(input("q:"))
e = int(input("e:"))
fn = (p-1) * (q-1) #计算欧拉函数
print(gmpy2.invert(e, fn))
```